

## Media Contact: Will Wiquist will.wiquist@fcc.gov

## For Immediate Release

## FCC CUTS OFF PROVIDER FROM NETWORK ACCESS FOR FAILING TO MEET ROBOCALL MITIGATION REQUIREMENTS

WASHINGTON, November 22, 2022—The Federal Communications Commission today announced that, for the first time, a voice service provider is being cut off from other networks for failing to meet the FCC's requirements for protecting consumers against scam robocalls and malicious caller ID spoofing. The FCC's Enforcement Bureau today ordered that Global UC be removed from the Robocall Mitigation Database which, as today's Order states, "requires all intermediate providers and terminating voice service providers to cease accepting the Company's traffic."

"For too long, robocalls have flooded our phones and facilitated fraud. So we are using a new tool to fight against these scam calls. We are cutting providers off and preventing them from accessing our networks when they fail to demonstrate they will protect consumers. This is a novel way to stop robocalls and it's one we are going to keep using until we get this junk off the line," said FCC Chairwoman Jessica Rosenworcel.

While Global UC is the first company to be removed, the FCC continues to review responses to "show cause" orders requiring specific other providers show their concrete steps taken to protect consumer from scam robocalls and spoofing.

"We have reached the point where we are ready to remove companies if they fail to abide by the rules and heed our warnings," said **Enforcement Bureau Chief Loyaan A. Egal**. "While this is a steep and impactful penalty, it underscores the importance we place on complying with our rules, which are designed to eliminate the ability of bad actors to use the U.S. communications networks to harm consumers."

Certification in the Robocall Mitigation Database requires implementation of STIR/SHAKEN caller ID authentication protocols and/or detailed robocall mitigation plans for any portions of their networks where STIR/SHAKEN cannot be implemented (e.g. non-IP networks). Database certification applicants that fail to meet the FCC's robocall mitigation standards receive notification from the FCC's Wireline Communication Bureau and, if they fail to respond and correct their filing, a "show cause" order from the Enforcement Bureau.

The FCC's Robocall Response Team – an agency-wide working group covering enforcement, spoofing and robocall policy-making, and more – has garnered results in protecting consumers:

- A "K4 Notice" authorizing all U.S.-based voice service providers to cease carrying specified traffic related to an auto warranty scam robocall campaign. This resulted in a massive, 99% drop in the volume of these calls since June, according to RoboKiller;
- A "K4 Notice" was recently <u>issued</u> against a student loan robocall campaign, following a consumer alert and Enforcement Advisory;
- STIR/SHAKEN standards have been widely implemented across IP networks;

- Record-breaking spoofing and robocall fines;
- Closing gateways used by international robocallers to reach Americans' phones;
- Signing robocall investigation partnerships with 43 states plus DC and Guam; and
- Launching a robotext proceeding to protect consumer from scam text messages.

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / Twitter: @FCC / www.fcc.gov

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).